WolfSSL

Luca Valentini

Insert Date

Contents

Abstract

This document is meant to be a small introductory guide to wolfssl.
For the creation of this thesis I used the official wolfssl manual and some github repository related to wolfssl.

Chapter 1

SSL Protocol

1.1 Introduction

The SSL protool is a client/server protocol that provides the following basic security services to the communicating peers:

- Authentication (both peer entity anda data origin authentication) services
- Connection confidentiality services
- Connection integrity services

The SSL protocol is sockets-oriented, meaning that all or none of the data that is sent to or received from a network connection is cryptographically protected in exactly the same way. It can be best viewed as an intermediate layer between the transporrt and the application layer that serves two purposes:

- Establish a secure connection between the commucating peers
- Use this connection to securely trasmit giher-layer protocol data from the sender to the reciever. It therefore fragments the data in pieces called fragments; each fragment is optionally compressed, authenticated, encrypted, prepended with a header, and transmitted to the reciever. Each data fragment prepared this way is sent in a distinct SSL record.

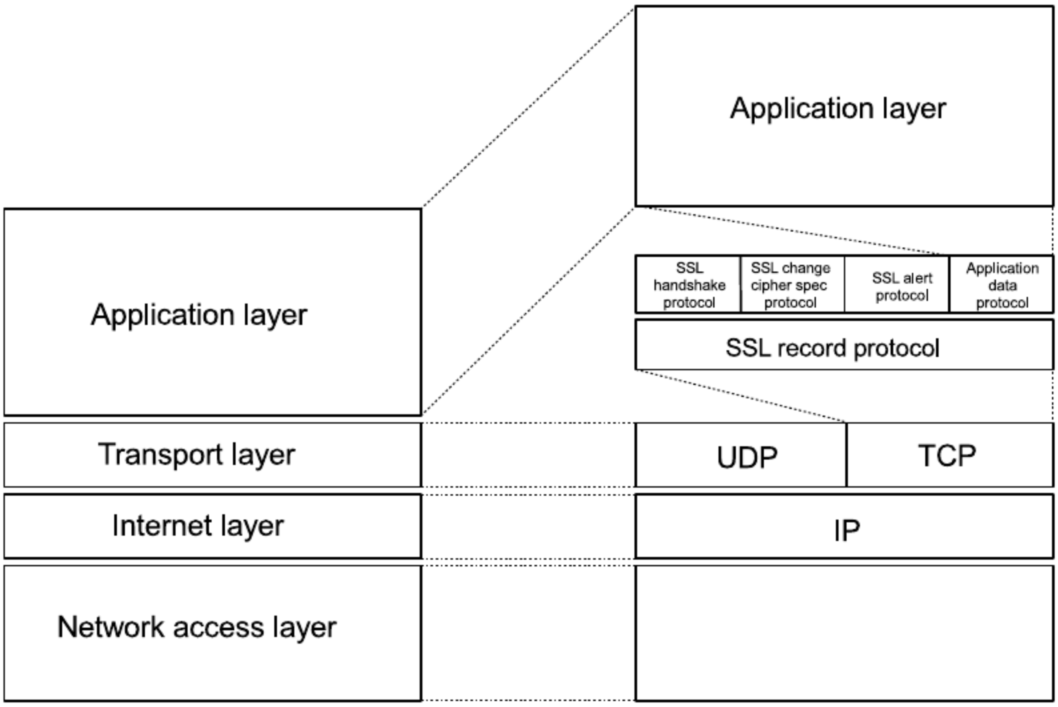


Figure 1.1: The SSL with its (sub)layer and (sub)protocols

The SSL consists of two sublayers and a few subprotocols:

- The lower sublayer is stacked on top of some connection-oriented and reliable transport layer protocol. This layer basically comprises the SSL record protocol that is used for the encapsulation of the higher-layer protocol data.

- The higher sublayer is stacked on top of the SSL record protocol and comprises four subprotocols.

  - The *SSL handshake protocol* is the core subprotocol of SSL. It is used for establishment of a secure connection. It allows the communicating peers to authenticate each other and to negotiate a cipher suite and a compression method.
  - The *SSL change cipher spec protocol* is used to put the parameters, set by the SSL handshake protocol in place and make them effective.
  - The *SSL alert protocol* allows the communicating peers to signal indicators of potential problems and send respective alert messages to each other.

– The *SSL application data protocol* is used for the secure transmission of application data.

In spite of the fact that SSL consists of several subprotocols, we use the term *SSL protocol* to refer to all of them simultaneously.

1.2 SSL Handshake

The SSL handshake protocol is layered on top of the SSL record protocol. It allows a client and server to authenticate each other and to negotiate issues like cipher suites and compression methods.

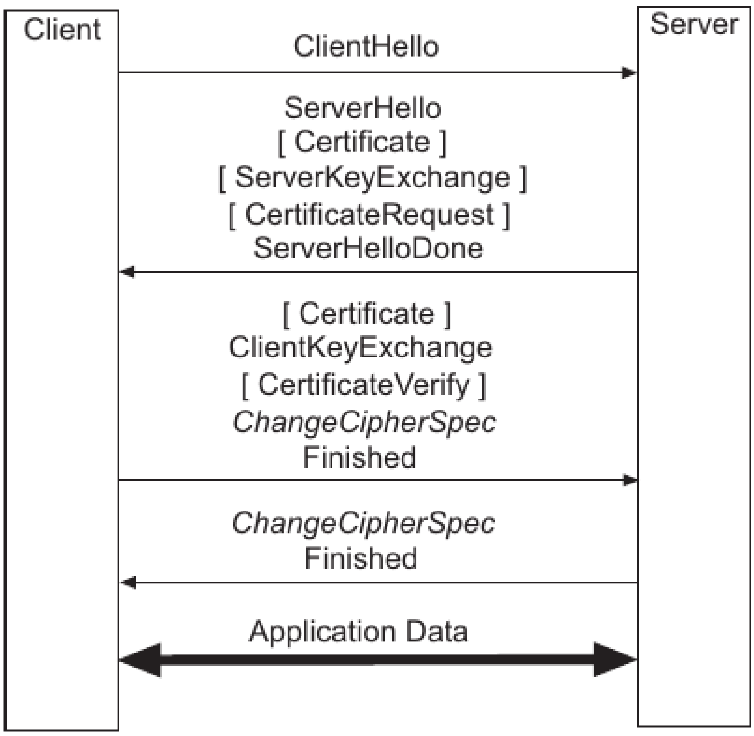


Figure 1.2: The SSL handshake protocol

The SSL handshake protocol comprises four sets of messages:

- The first flight comprises a single *ClientHello* message that is sent from the client to the server.

- The second flight comprises two messages that are sent back from the server to the client:

  1. *ServerHello* message is sent in response to the *ClientHello* message
  2. (optional) If the server is to authenticate itself, it may send a *Certificate* message to the client.
  3. (optional) Under some circumstances, the server may send a *ServerKeyExchange* message to the client.
  4. (optional) If the server requires the client to authenticate itself with a public key certificate, then it may send a *CertificateRequest* message to the client.
  5. Finally, server send a *ServerHelloDone* message to the client.

- The third flight comprises three to five messages that are again sent from the client to the server:

  1. (optional) If the server has sent a *CertificateRequest* message, then the client sends a *Certificate* message to the server.
  2. In the main step of the protocol, the client sends a *ClientKeyExchange* message to the server.
  3. (optional) If the client has sent a certificate to the server, then it must also send a *CertificateVerify* message to the server. This message is digitally signed with the private key that corresponds to the client certificate's public key.
  4. The client sends a *ChangeCipherSpec* message to the server (using the SSL change cipher spec protocol) and copies its pending write state into the current write state.
  5. The client sends a *Finished* message to the server. As mentioned above, this is the first message that is cryptographically protected under the new cipher spec.

- The fourth flight comprises two messages that are sent from the server back to the client:

  1. The server sends another *ChangeCipherSpec* message to the client and copies its pending write state into the current write state.
  2. Finally, the server send a *Finished* message to the client. Again, this message is cryptographically protected under the new cipher spec.

At this point in time, the SSL handshake is complete and the client and server may start exchanging application-layer data.

Chapter 2

WolfSSL

The wolfSSL embedded SSL library is a lightweight SSL/TLS library written in ANSI C and targeted for embedded, RTOS, and resource-constrained environments - primarily because of its small size, speed, and feature set; It's an SSL/TLS library optimized to run on embedded platforms.
It's free and it has an excellent cross platform support.
WolfSSL supports standards up to the current TLS 1.3 and DTLS 1.2 levels, is up to 20 times smaller than OpenSSL and it's powered by the colfCrypt library.

This library is built for maximum portability and supports the C programming language as a primary interface. It also supports several other host languages, including Java (wolfSSL JNI), C# (wolfSSL C#), Python, and PHP and Perl.

To improve performance it supports hardware cryptography and acceleration on several platforms.

In the following list you can see some of WolfSSI's features:

- Runtime memory usage between 1-36 kB
- OpenSSl compatibility layer
- Hash Functions:
  - MD2
  - MD4
  - MD5
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512
  - BLAKE2b
  - RIPEMD-160
  - Poly1305

- Mutual authentication support (client/server)
- SSL Sniffer (SSL Inspection) Support
- IPv4 and IPv6 support

The operating systems supported are:

1. Win32/64
2. Linux
3. Mac OS X
4. Solaris
5. ThreadX
6. VxWorks
7. FreeBSD
8. NetBSD
9. OpenBSD
10. embedded Linux
11. Yocto Linux
12. OpenEmbedded
13. WinCE
14. Haiku
15. OpenWRT
16. iPhone(iOS)
17. Android
18. Nintendo Wii and Gamecube through DevKitPro
19. QNX
20. MontaVista
21. NonStop
22. TRON / ITRON / ITRON
23. Micrium C / OS - III
24. FreeRTOS
25. SafeRTOS
26. NXP / Freescale MQX
27. Nucleus
28. TinyOS
29. HP / UX
30. AIX
31. ARC MQX
32. TI - RTOS
33. uTasker
34. embOS
35. INtime
36. Mbed
37. uT - Kernel
38. RIOT
39. CMSIS -RTOS
40. FROSTED
41. Green Hills INTEGRITY
42. Keil RTX
43. TOPPERS
44. PetaLinux
45. Apache Mynewt
46. PikeOS

Chapter 3

Test case

3.1 Client/Server provided by WolSSL

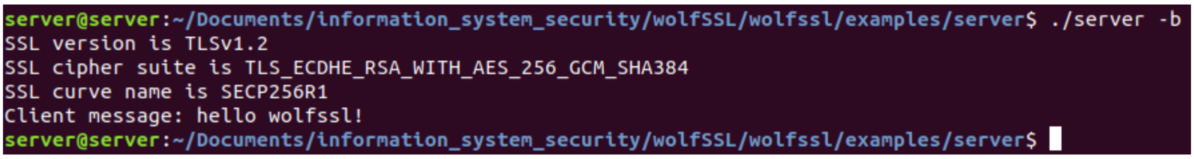


Figure 3.1: Server SSL

+

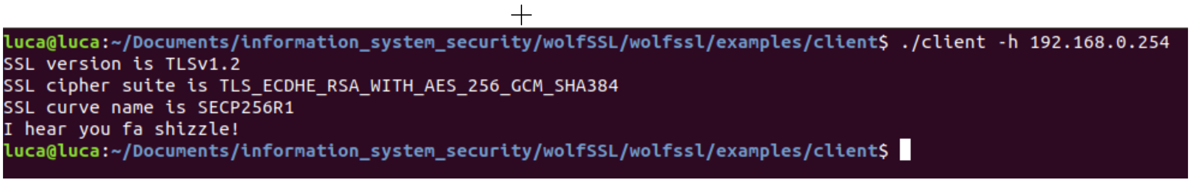
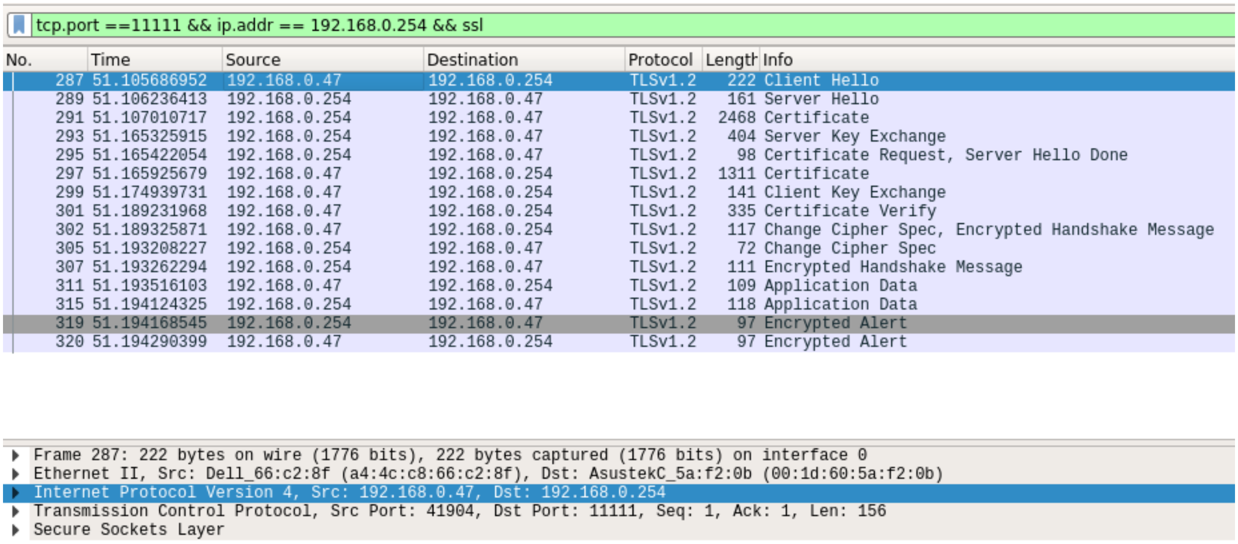


Figure 3.2: Client SSL

In this example, the server is a simple SSL server that allows only one client connection; after the connection with a client, the server receives an encrypted message from client, it responds and quits.
The -b parameter allows the server to bind to any interface instead of localhost only.

The client after the connection with the server, sends a message (hello wolfssl!) and after the server response, it quits.
The -h parameter allows the client to specify the server address to perform the connection.



tcp.port ==11111 && ip.addr == 192.168.0.254 && ssl

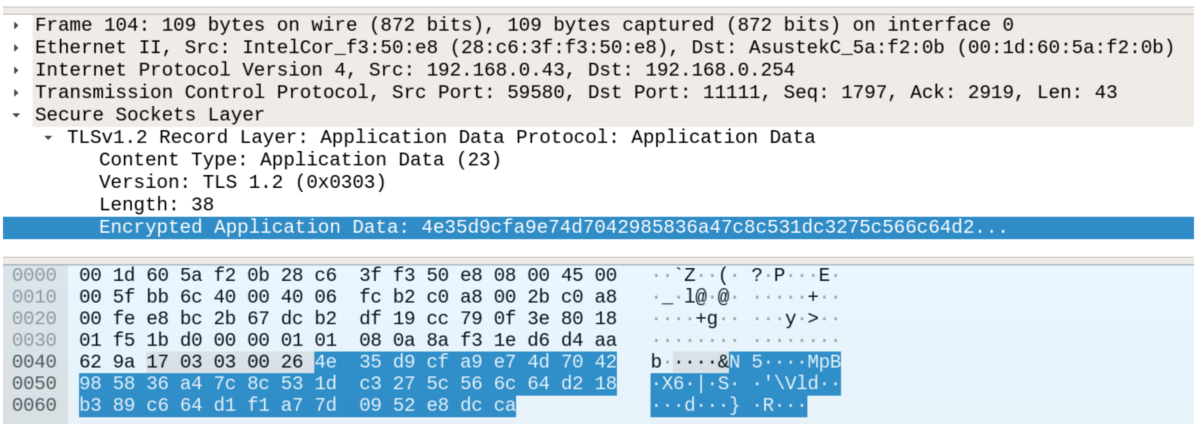
No.	Time	Source	Destination	Protocol	Length	Info
287	51.105686952	192.168.0.47	192.168.0.254	TLSv1.2	222	Client Hello
289	51.106236413	192.168.0.254	192.168.0.47	TLSv1.2	161	Server Hello
291	51.107010717	192.168.0.254	192.168.0.47	TLSv1.2	2468	Certificate
293	51.165325915	192.168.0.254	192.168.0.47	TLSv1.2	404	Server Key Exchange
295	51.165422054	192.168.0.254	192.168.0.47	TLSv1.2	98	Certificate Request, Server Hello Done
297	51.165925679	192.168.0.47	192.168.0.254	TLSv1.2	1311	Certificate
299	51.174939731	192.168.0.47	192.168.0.254	TLSv1.2	141	Client Key Exchange
301	51.189231968	192.168.0.47	192.168.0.254	TLSv1.2	335	Certificate Verify
302	51.189325871	192.168.0.47	192.168.0.254	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
305	51.193208227	192.168.0.254	192.168.0.47	TLSv1.2	72	Change Cipher Spec
307	51.193262294	192.168.0.254	192.168.0.47	TLSv1.2	111	Encrypted Handshake Message
311	51.193516103	192.168.0.47	192.168.0.254	TLSv1.2	109	Application Data
315	51.194124325	192.168.0.254	192.168.0.47	TLSv1.2	118	Application Data
319	51.194168545	192.168.0.254	192.168.0.47	TLSv1.2	97	Encrypted Alert
320	51.194290399	192.168.0.47	192.168.0.254	TLSv1.2	97	Encrypted Alert

Frame 287: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits) on interface 0
Ethernet II, Src: Dell_66:c2:8f (a4:4c:c8:66:c2:8f), Dst: AsustekC_5a:f2:0b (00:1d:60:5a:f2:0b)
Internet Protocol Version 4, Src: 192.168.0.47, Dst: 192.168.0.254
Transmission Control Protocol, Src Port: 41904, Dst Port: 11111, Seq: 1, Ack: 1, Len: 156
Secure Sockets Layer

Figure 3.3: All SSL packets sent

Client IP: 192.168.0.47 Server IP: 192.168.0.254

Come si puo' bene vedere dalla figura soprastante, la comunicazione viene iniziata dal client con un 'Client Hello'; dopo SSL handshake, ci sono due messaggi 'Application Data' inviati rispettivamente dal client verso il server e dal server verso il client il cui contenuto e' cifrato. Una volta che il server invia la risposta al client, la comunicazione viene chiusa attraverso 'Encrypted Alert'.



```
Frame 104: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface 0
Ethernet II, Src: IntelCor_f3:50:e8 (28:c6:3f:f3:50:e8), Dst: AsustekC_5a:f2:0b (00:1d:60:5a:f2:0b)
Internet Protocol Version 4, Src: 192.168.0.43, Dst: 192.168.0.254
Transmission Control Protocol, Src Port: 59580, Dst Port: 11111, Seq: 1797, Ack: 2919, Len: 43
Secure Sockets Layer
  TLSv1.2 Record Layer: Application Data Protocol: Application Data
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 38
    Encrypted Application Data: 4e35d9cfa9e74d7042985836a47c8c531dc3275c566c64d2...

0000  00 1d 60 5a f2 0b 28 c6  3f f3 50 e8 08 00 45 00   ··`Z··(· ?·P···E·
0010  00 5f bb 6c 40 00 40 06  fc b2 c0 a8 00 2b c0 a8   ·_·l@·@· ·····+··
0020  00 fe e8 bc 2b 67 dc b2  df 19 cc 79 0f 3e 80 18   ····+g·· ···y·>··
0030  01 f5 1b d0 00 00 01 01  08 0a 8a f3 1e d6 d4 aa   ········ ········
0040  62 9a 17 03 03 00 26 4e  35 d9 cf a9 e7 4d 70 42   b·····&N 5····MpB
0050  98 58 36 a4 7c 8c 53 1d  c3 27 5c 56 6c 64 d2 18   ·X6·|·S· ·'\Vld··
0060  b3 89 c6 64 d1 f1 a7 7d  09 52 e8 dc ca            ···d···} ·R···
```

Figure 3.4: Content of the encrypted message

Come si puo' vedere, lo scambio di messaggi e' cifrato.

3.2 EchoClient/EchoServer provided by WolfSSL

```
luca@luca:~/Documents/information_system_security/wolfSSL/wolfssl/examples/echoserver$ ./echoserver
Hi Server, I'm echoClient!
client sent quit command: shutting down!
luca@luca:~/Documents/information_system_security/wolfSSL/wolfssl/examples/echoserver$
```

Figure 3.5: EchoServer SSL

```
luca@luca:~/Documents/information_system_security/wolfSSL/wolfssl/examples/echoclient$ ./echoclient
Hi Server, I'm echoClient!
Hi Server, I'm echoClient!
quit
sending server shutdown command: quit!
luca@luca:~/Documents/information_system_security/wolfSSL/wolfssl/examples/echoclient$
```

Figure 3.6: EchoClient SSL

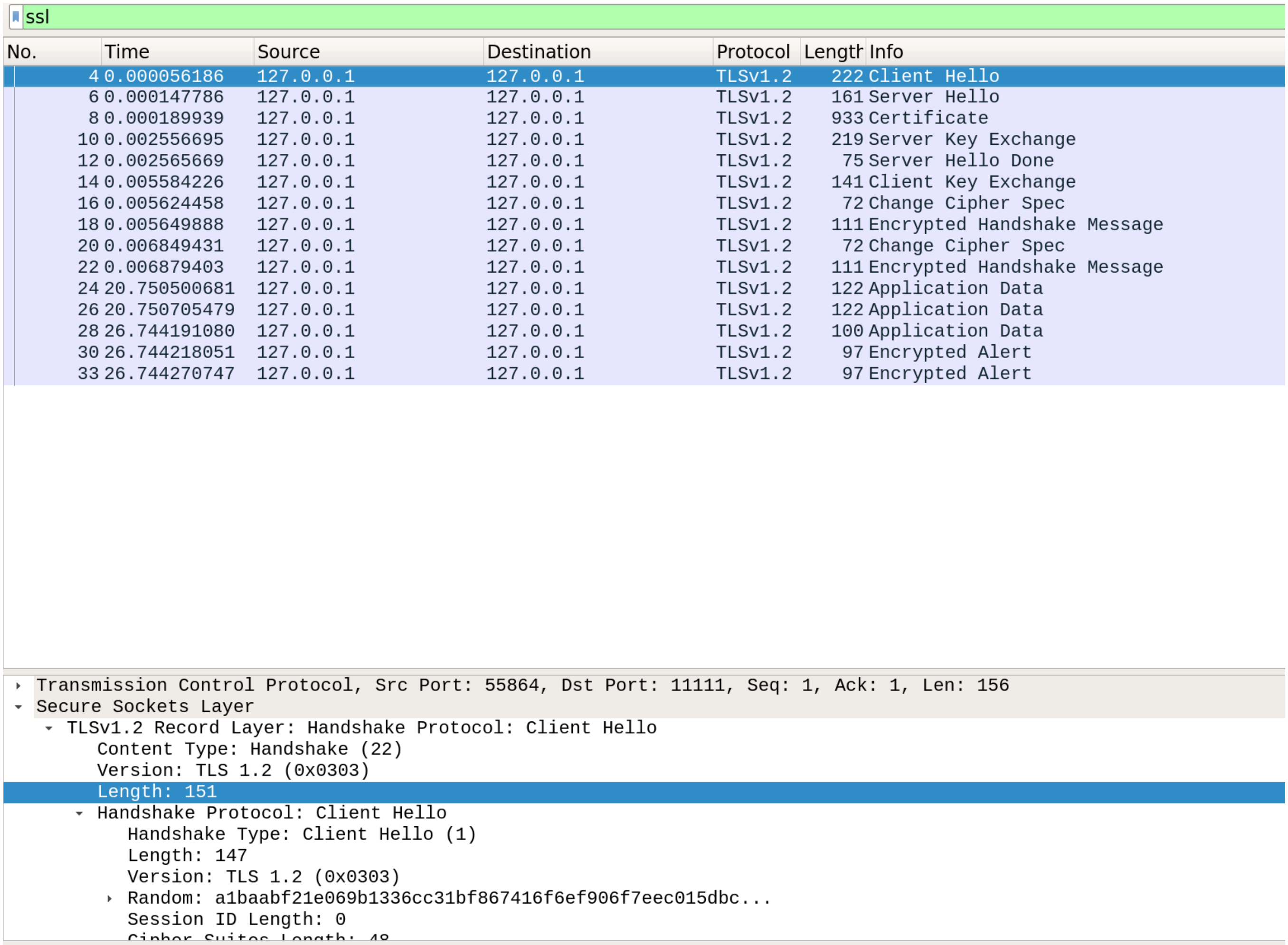


Figure 3.7: All SSL packets sent

Chapter 4

Create a program using WolfSSL

4.1 TCP application

To create an SSL program you can modify your TCP program added several SSL functions. To explain the migration from TCP to SSL, I created a simple chat between a client and a server available on github.

4.2 From TCP to SSL

To create a wolfSSL application the first thing that I did is include the wolfSSL API header in your program.

```
#include <wolfssl/ssl.h>
```

After the inclusion of the header files, I initialize the library and the WOLFSSL_CTX calling **wolfSSL_Init**; This is necessary to use the library.

The WOLFSSL_CTX structure contains global values for each SSL connection, including certificate information. To create a new WOLFSSL_CTX there is **wolfSSL_CTX_new()** function. it requires an argument which defines the SSL or TLS protocol for the client or server to use. In my case I used TLS 1.3, so the call is:

```
WOLFSSL_CTX *ctx = wolfSSL_CTX_new(wolfTLSv1_3_server_method());
```

for the server;

```
WOLFSSL_CTX *ctx = wolfSSL_CTX_new(wolfTLSv1_3_client_method())
```

for the client.

In the WOLFSSL_CTX can be loaded the CA (Certificate Authority) so that the client is able to verify the server's identity when they start the connection. To load the CA into the WOLFSSL_CTX there is **wolfSSL_CTX_load_verify_locations()**. This function requires three arguments:

- a WOLFSSL_CTX pointer
- a certificate file
- a path value that point to a directory which should contain CA certificates in PEM format.

this function returns SSL_SUCCESS or SSL_FAILURE.
wolfSSL_CTX_load_verify_locations() can be used for verify the client or the server identity, but in my case, only the client loads the CA, the server loads a certificate file into the SSL context (WOLFSSL_CTX) calling:

```
int wolfSSL_CTX_use_certificate_file(ctx, CERT_FILE,
    SSL_FILETYPE_PEM);
```

Also the server private key can be loaded using the wolfSSL library; the function is:

```
int wolfSSL_CTX_use_PrivateKey_file(ctx, KEY_FILE,
    SSL_FILETYPE_PEM)
```

After a TCP connection the WOLFSSL object needs to be created and the file descriptor needs to be associated with the session; the instructions are:

```
//Connect to socket file descriptor
WOLFSSL* ssl;
//create WOLFSSL object
ssl = wolfSSL_new(ctx);
wolfSSL_set_fd(ssl,sockfd);
```

After the previous instructions called by client and server, the server waits an SSL client to initiate the SSL handshake; it waits until a client call **wolfSSL_connect(ssl)** and then the handshake starts.

Once the connection functions are set, I replaced **read(...)** function with:

```
int wolfSSL_read(WOLFSSL *ssl, void *data, int sz);
```

It read **sz** bytes from the SSL session **ssl** internal read buffer into the buffer **data**. The bytes are removed from the internal receive buffer;

Instead the **write(...)** function is replaced by:

```
int wolfSSL_write(WOLFSSL *ssl, void *data, int sz);
```

It writes **sz** bytes from the buffer, **data**, to the SSL connection, **ssl**.

When the application is over, the WOLFSSL_CTX object and the wolfSSL library must be freed; the instructions are:

```
wolfSSL_free(ssl);
wolfSSL_CTX_free(ctx);
wolfSSL_Cleanup();
```

4.3 SSL application

To develop an SSL application, I started from the TCP chat explained in the previous section and I added the wolfSSL function to create an encrypted communication.
The goal of this program is to show how to create a simple encrypted chat, focusing on the security of an application and not to the good practices of the socket and thread applications.
Some part of the code like inclusion and global variables are omitted (wolfSSL object and other variables are stored in global memory); you can find them on github.
In the next subsections I'll try to explain the code of the program:

4.3.1 SSL Server

The server created by me authenticate itself by sending a certificate; For testing purpose, all the certificates that I use, I took from wolfSSL download. It also use an RSA key for secure symmetric key exchange that is used for actual transmitted data encryption and decryption.
After the initialization of the wolfSSL and the socket, the main function marks the socket referred to by sockfd as a passive socket, that is, as a socket that will be used to accept incoming connection requests using accept.

```
int main()
{
    int ret;

    /* Initialize wolfSSL */
    wolfSSL_Init();

    /* Create a socket that uses an internet IPv4 address,
     * Sets the socket to be stream based (TCP),
     * 0 means choose the default protocol. */
    if ((sockfd = socket(AF_INET, SOCK_STREAM, 0)) == -1)
    {
        fprintf(stderr, "ERROR: failed to create the socket\n");
        return -1;
    }
    /* Create and initialize WOLFSSL_CTX */

    if ((ctx = wolfSSL_CTX_new(wolfTLSv1_3_server_method())) ==
        NULL)
```

```
{
    fprintf(stderr, "ERROR: failed to create WOLFSSL_CTX\n");
    return -1;
}

/* Load server certificates into WOLFSSL_CTX */
if (wolfSSL_CTX_use_certificate_file(ctx, CERT_FILE,
    SSL_FILETYPE_PEM) != SSL_SUCCESS)
{
    fprintf(stderr, "ERROR: failed to load %s, please check the
        file.\n",
            CERT_FILE);
    return -1;
}

/* Load server key into WOLFSSL_CTX */
if (wolfSSL_CTX_use_PrivateKey_file(ctx, KEY_FILE,
    SSL_FILETYPE_PEM) != SSL_SUCCESS)
{
    fprintf(stderr, "ERROR: failed to load %s, please check the
        file.\n",
            KEY_FILE);
    return -1;
}

/* Initialize the server address struct with zeros */
memset(&servAddr, 0, sizeof(servAddr));

/* Fill in the server address */
servAddr.sin_family = AF_INET;        /* using IPv4    */
servAddr.sin_port = htons(DEFAULT_PORT); /* on DEFAULT_PORT */
servAddr.sin_addr.s_addr = INADDR_ANY; /* from anywhere */

/* Bind the server socket to our port */
if (bind(sockfd, (struct sockaddr *)&servAddr,
    sizeof(servAddr)) == -1)
{
    fprintf(stderr, "ERROR: failed to bind\n");
    return -1;
}

/* Listen for a new connection*/
if (listen(sockfd, 1) == -1)
```

```
    {
        fprintf(stderr, "ERROR: failed to listen\n");
        return -1;
    }
   .
   .
   .
```

Listing 4.1: int main() of SSL server, 1* part

This server can communicate with one client at a time so there is an infinite loop where the encrypted connection with a client is established. At this point a mainThread is created to handle reading and writing through the secure channel. Whenever the connection falls, the thread ends and the server try to established a new connection. The server ends only when keyboard of the server type 'quit' (this part is in another function).

```
    /* Continue to accept clients until shutdown is issued */
    while (1)
    {
       printf("Waiting for a connection...\n");
        /* Accept client connections */
        if ((connd = accept(sockfd, (struct sockaddr *)&clientAddr,
            &size)) == -1)
        {
            fprintf(stderr, "ERROR: failed to accept the
                connection\n\n");
            return -1;
        }

        /* Create a WOLFSSL object */
        if ((ssl = wolfSSL_new(ctx)) == NULL)
        {
            fprintf(stderr, "ERROR: failed to create WOLFSSL
                object\n");
            return -1;
        }

        /* Attach wolfSSL to the socket */
        wolfSSL_set_fd(ssl, connd);

        /* Establish TLS connection */
        ret = wolfSSL_accept(ssl);
        if (ret != SSL_SUCCESS)
```

```c
        {
            fprintf(stderr, "wolfSSL_accept error = %d\n",
                    wolfSSL_get_error(ssl, ret));
            return -1;
        }

        printf("Client connected successfully\n");
        pthread_t mainThread;
        pthread_create(&mainThread, NULL, ClientHandler, NULL);
        pthread_join(mainThread, NULL);
        printText("Communication is ended!\n", "System");

        if (is_end)
            break;
    }
    ncurses_end();
    printf("Shutdown complete\n");

    /* Cleanup after this connection */
    wolfSSL_free(ssl); /* Free the wolfSSL object        */
    close(connd);     /* Close the connection to the client */
    /* Cleanup and return */
    wolfSSL_CTX_free(ctx); /* Free the wolfSSL context object   */
    wolfSSL_Cleanup();   /* Cleanup the wolfSSL environment     */
    close(sockfd);       /* Close the socket listening for clients
        */
    return 0;            /* Return reporting a success          */
}
```

Listing 4.2: int main() of SSL server, 2* part

The previously created thread executes ClientHandler function; even if the connection is established, it shows 'Client name connected successfully' message on the screen only after reading the username from the secure channel.
After that two thread are created, one for read messages and one for write messages.

```c
void *ClientHandler(void *args)
{
    int ret;
    /*********************** USERNAME */
    /* Read the client username into our buff array */
    XMEMSET(buff, 0, sizeof(buff));
```

```
    ret = wolfSSL_read(ssl, buff, sizeof(buff) - 1);
    ncurses_start();
    clearWin();
    if (ret > 0)
    {
        /* Print to stdout any data the client sends */
        strcpy(username, buff);
        char text[256];
        sprintf(text, "Client %s connected successfully", username);
        printText(text, "System");
        printText("****************************\n", "System");
        fflush(stdout);
    }
    else
    {
        printText("ERROR!!", "System");
        close(sockfd);    /* Close the connection to the server */
        pthread_exit(NULL); /* End theread execution          */
    }
    /**************************** */
    XMEMSET(buff, 0, sizeof(buff));

    if (pthread_create(&Treader, NULL, readBuffer, NULL))
    {
        fprintf(stderr, "Error creating thread\n");
        fflush(stdout);
        return NULL;
    }

    if (pthread_create(&Twriter, NULL, writeBuffer, NULL))
    {
        fprintf(stderr, "Error creating thread\n");
        fflush(stdout);
        return NULL;
    }

    pthread_join(Treader, NULL);
    pthread_join(Twriter, NULL);
    /* Cleanup after this connection */
    close(connd);     /* Close the connection to the client */
    pthread_exit(NULL); /* End theread execution          */
}
```

Listing 4.3: ClientHandler() of SSL server

WriteBuffer is a function executes by a thread for writing in the channel. **read_in()** read the characters typed from the user until a new line and then sent the message with **wolfSSL_write(ssl,Rbuffer,len)**.

```
void *writeBuffer(void *args)
{
    int ret;
    while (1)
    {
        read_in();
        len = XSTRLEN(Rbuffer);

        /* Reply back to the client */
        do
        {
            ret = wolfSSL_write(ssl, Rbuffer, len);
            /* TODO: Currently this thread can get stuck infinitely
                if client
         *      disconnects, add timer to abort on a timeout
            eventually,
         *      just an example for now so allow for possible stuck
            condition
         */
            printText(Rbuffer, "Server");

        } while (wolfSSL_want_write(ssl));

        if (XSTRNCMP(Rbuffer, "quit", 4) == 0)
        {
            is_end = 1;
            break;
        }

        if (ret != len)
        {
            printText("ERROR!!", "System");
            break;
        }
    }
    pthread_cancel(Treader);
```

```
    return NULL;
}
```

Listing 4.4: writeBuffer() of SSL server

ReadBuffer function read messages from the channel through **wolfSSL_read(ssl, buffReader, sizeof(buffReader)-1)**. If the user on the other side writes 'quit', this function and writeBuffer function end.

```
void *readBuffer(void *args)
{
    int ret;
    while (1)
    {
        /* Read the client data into our buff array */
        XMEMSET(buffReader, 0, sizeof(buffReader));
        ret = wolfSSL_read(ssl, buffReader, sizeof(buffReader) - 1);

        if (ret > 0)
        {
            if (!strcmp(buffReader, "quit"))
            {
                pthread_cancel(Twriter);
                pthread_exit(NULL); /* End theread execution
                            */
            }
            printText(buffReader, username);
        }
        else
        {
            printText("ERROR READ!!", "System");
            pthread_cancel(Twriter);
            pthread_exit(NULL); /* End theread execution          */
        }
    }
}
```

Listing 4.5: readBuffer() of SSL server

4.3.2 SSL Client

The SSL client has 3 thread; The main thread called Tclient that is used to manage read and write threads.
To execute the SSL client, the program needs the IP address of server. If the user doesn't provide it during the program calls, the program ends.

```c
int main(int argc, char **argv)
{
    pthread_t Tclient;
    /* Check for proper calling convention */
    if (argc != 2)
    {
        printf("usage: %s <IPv4 address>\n", argv[0]);
        return -1;
    }
    ip = argv[1];
    /* create a second thread which executes inc_x(&x) */
    if (pthread_create(&Tclient, NULL, client, NULL))
    {
        fprintf(stderr, "Error creating thread\n");
        fflush(stdout);
        return 1;
    }
    if (pthread_join(Tclient, NULL))
    {
        fprintf(stderr, "Error joining thread\n");
        return 2;
    }
    ncurses_end();
    return 0; /* Return reporting a success          */
}
```

Listing 4.6: int main() of SSL client

As in the server part, the function below is executed by a thread; it initializes WOLFSSL objects, socket etc. After initializations the function tries to connect to the secure channel, through the IP address inserted at the execution of the client.

```c
void *client(void *args)
{
    struct sockaddr_in servAddr;
```

```
printf("Set your username: ");
refresh();
if (!scanf("%s", username))
{
    fprintf(stderr, "ERROR: failed to get message for
        server\n");
    return NULL;
}
ncurses_start();
/* Initialize wolfSSL */
wolfSSL_Init();

/* Create a socket that uses an internet IPv4 address,
 * Sets the socket to be stream based (TCP),
 * 0 means choose the default protocol. */
if ((sockfd = socket(AF_INET, SOCK_STREAM, 0)) == -1)
{
    fprintf(stderr, "ERROR: failed to create the socket\n");
    return NULL;
}

/* Create and initialize WOLFSSL_CTX */
if ((ctx = wolfSSL_CTX_new(wolfTLSv1_3_client_method())) ==
    NULL)
{
    fprintf(stderr, "ERROR: failed to create WOLFSSL_CTX\n");
    return NULL;
}

/* Load client certificates into WOLFSSL_CTX */
if (wolfSSL_CTX_load_verify_locations(ctx, CERT_FILE, NULL) !=
    SSL_SUCCESS)
{
    fprintf(stderr, "ERROR: failed to load %s, please check the
        file.\n",
            CERT_FILE);
    return NULL;
}

/* Initialize the server address struct with zeros */
memset(&servAddr, 0, sizeof(servAddr));

/* Fill in the server address */
```

```c
servAddr.sin_family = AF_INET;        /* using IPv4    */
servAddr.sin_port = htons(DEFAULT_PORT); /* on DEFAULT_PORT */

/* Get the server IPv4 address from the command line call */
if (inet_pton(AF_INET, ip, &servAddr.sin_addr) != 1)
{
    fprintf(stderr, "ERROR: invalid address\n");
    return NULL;
}

/* Connect to the server */

if (connect(sockfd, (struct sockaddr *)&servAddr,
    sizeof(servAddr)) == -1)
{
    printText("ERROR: failed to connect", "System");
    return NULL;
}
/*Do something*/

/* Create a WOLFSSL object */
if ((ssl = wolfSSL_new(ctx)) == NULL)
{
    fprintf(stderr, "ERROR: failed to create WOLFSSL object\n");
    return NULL;
}

/* Attach wolfSSL to the socket */
wolfSSL_set_fd(ssl, sockfd);
/* Connect to wolfSSL on the server side */
if (wolfSSL_connect(ssl) != SSL_SUCCESS)
{
    fprintf(stderr, "ERROR: failed to connect to wolfSSL\n");
    return NULL;
}

strtok(username, "\n");
len = strnlen(username, sizeof(username));
/* Send the username to the server */
if (wolfSSL_write(ssl, username, len) != len)
{
    fprintf(stderr, "ERROR: failed to write\n");
    return NULL;
```

```
    }

    if (pthread_create(&Twriter, NULL, writeBuffer, NULL))
    {
        fprintf(stderr, "Error creating thread\n");
        fflush(stdout);
        return NULL;
    }

    if (pthread_create(&Treader, NULL, readBuffer, NULL))
    {
        fprintf(stderr, "Error creating thread\n");
        fflush(stdout);
        return NULL;
    }

    pthread_join(Twriter, NULL);
    pthread_cancel(Treader);
    pthread_join(Treader, NULL);

    /* Cleanup and return */
    wolfSSL_free(ssl);    /* Free the wolfSSL object                  */
    wolfSSL_CTX_free(ctx); /* Free the wolfSSL context object         */
    wolfSSL_Cleanup();    /* Cleanup the wolfSSL environment          */
    close(sockfd);        /* Close the connection to the server       */
    printText("Communication is ended!\n Press a button!!!",
        "System");
    getch();
    return NULL;
}
```

Listing 4.7: void *client(void *args) of SSL client

Reading and writing threads are similar to the server part, so I'm not putting them in this part.

4.4 Compile a WolfSSL program

To execute a wolfSSL program you must have installed wolfSSL on your pc, and then you must add **-lwolfssl** on your gcc command.
Me having used the threads and ncurses I have to add other flags to gcc command; to optimize the compilation I created a makefile.

4.5 Execute a WolfSSL program

In my project I used a laptop for the client part, and a Raspberry Pi for the server part; they are connected to the same LAN.
Below you can see the GUI of the client and the server part and the traffic analyze with wireshark.
The IP address of server is **192.168.0.53** and the port is **11111**.
The IP address of client is **192.168.0.46**

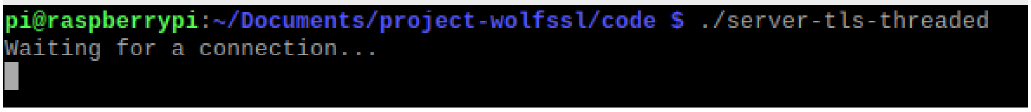


Figure 4.1: Execute WolfSSL server

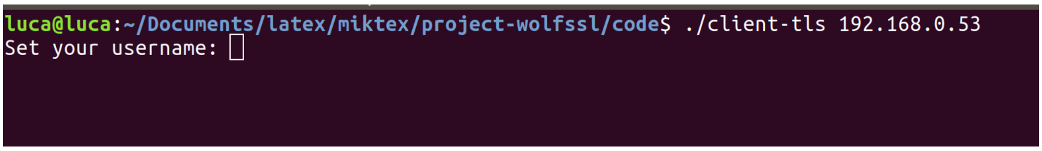


Figure 4.2: Execute WolfSSL client

After the execution of the server, a client can connect to it and the ssl handshake starts.
With the hello packet below, the client provides an ordered list of 27 cipher suites that it will support for encryption. The list is in the order preferred by the client, with highest preference first. This list can be modified by the programmer.
In this case, the client provides a list of optional extension which the server can use to take action or enable new features, for example:

- key_share
  - the client sends one or more public keys using an algorithm that it thinks the server will support. This allows the rest of the handshake after the ClientHello message to be encrypted.
- supported_version
  - the client indicates its support of TLS 1.3

No.	Time	Source	Destination	Protocol	Length	Info
8134	473.927206832	192.168.0.46	192.168.0.53	TLSv1.3	312	Client Hello
8136	473.954519818	192.168.0.53	192.168.0.46	TLSv1.3	194	Server Hello

```
▸ Frame 8134: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface wlp60s0, id 0
▸ Ethernet II, Src: IntelCor_f3:50:e8 (28:c6:3f:f3:50:e8), Dst: Raspberr_95:30:37 (dc:a6:32:95:30:37)
▸ Internet Protocol Version 4, Src: 192.168.0.46, Dst: 192.168.0.53
▸ Transmission Control Protocol, Src Port: 57618, Dst Port: 11111, Seq: 1, Ack: 1, Len: 246
▾ Transport Layer Security
  ▾ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 241
    ▾ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 237
        Version: TLS 1.2 (0x0303)
        Random: 415c66d8436758a9fb3260734a5ceb75cff9523aa7a1e07d…
        Session ID Length: 0
        Cipher Suites Length: 54
      ▸ Cipher Suites (27 suites)
        Compression Methods Length: 1
      ▸ Compression Methods (1 method)
        Extensions Length: 142
      ▾ Extension: key_share (len=71)
          Type: key_share (51)
          Length: 71
        ▾ Key Share extension
            Client Key Share Length: 69
          ▾ Key Share Entry: Group: secp256r1, Key Exchange length: 65
              Group: secp256r1 (23)
              Key Exchange Length: 65
              Key Exchange: 044b90c64339831bce6dc1d731dfda8f59ee518ad9b04ad8…
      ▾ Extension: supported_versions (len=3)
          Type: supported_versions (43)
          Length: 3
          Supported Versions length: 2
          Supported Version: TLS 1.3 (0x0304)
      ▾ Extension: signature_algorithms (len=32)
          Type: signature_algorithms (13)
          Length: 32
          Signature Hash Algorithms Length: 30
        ▸ Signature Hash Algorithms (15 algorithms)
      ▾ Extension: supported_groups (len=16)
          Type: supported_groups (10)
          Length: 16
          Supported Groups List Length: 14
        ▸ Supported Groups (7 groups)
      ▾ Extension: encrypt_then_mac (len=0)
          Type: encrypt_then_mac (22)
          Length: 0
```

Figure 4.3: Client Hello

In the Server Hello packet, the server has selected cipher suite 0x1301 (TLS_AES_128_GCM_SHA256) from the list of options given by the client. The server sends also a public key using the algorithm of the public key sent by the client. Once this is sent encryption keys can be calculated and the rest of the handshake will be encrypted. The rest of the packets are encrypted.

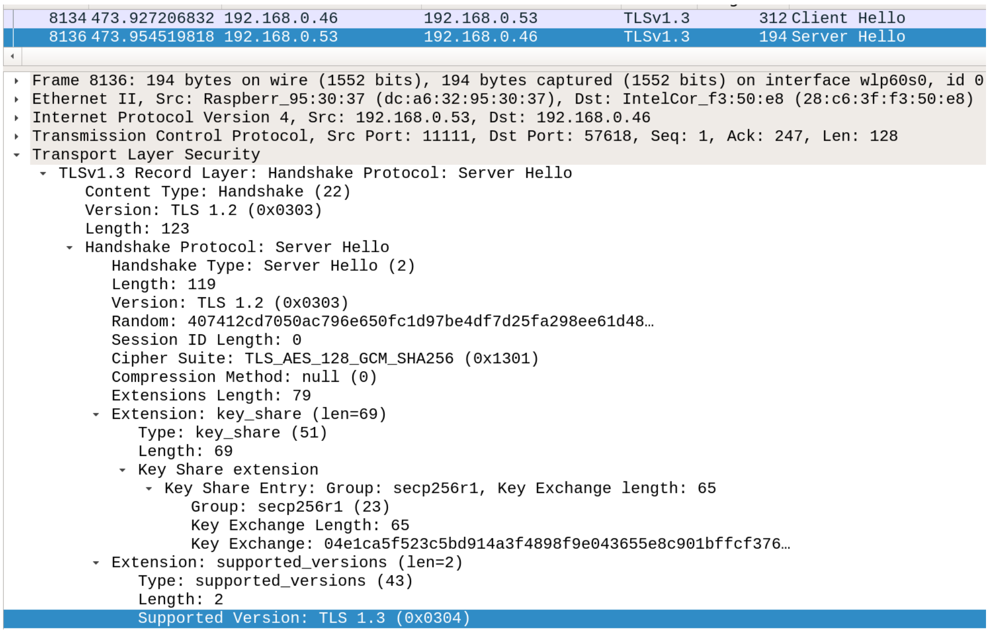


Figure 4.4: Server Hello

After the SSL handshake the situation in the server GUI is:

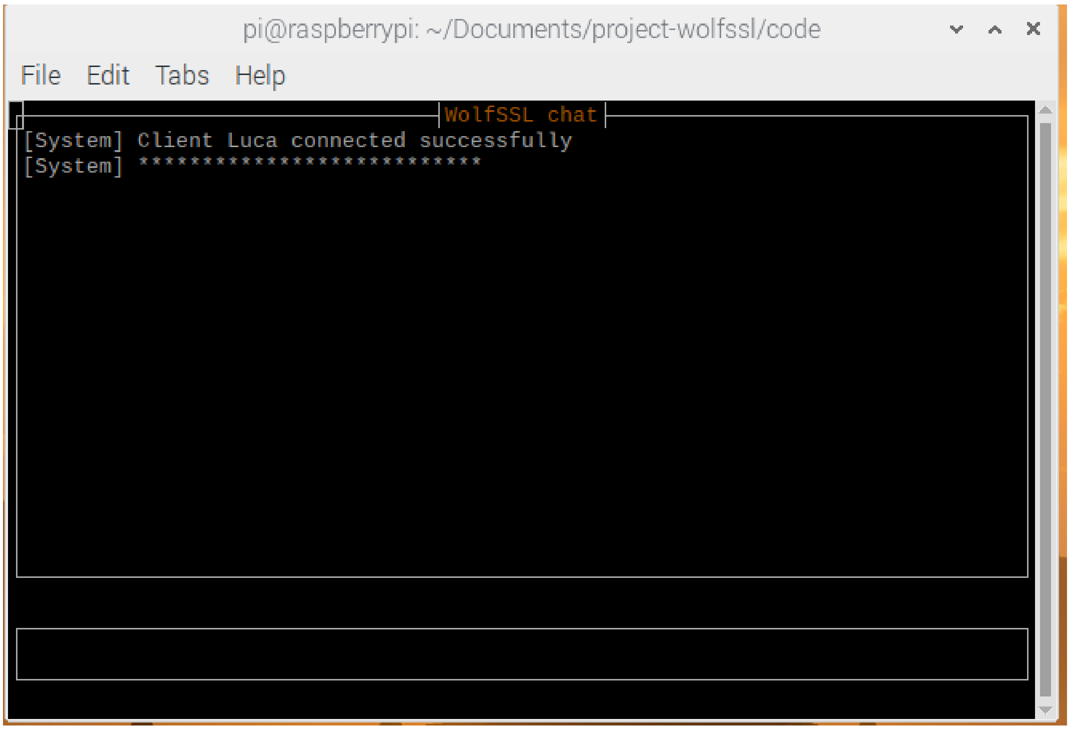


Figure 4.5: Client connected, server GUI

To test the exact function of the programs, I sent several messages between the laptop and the raspberry:

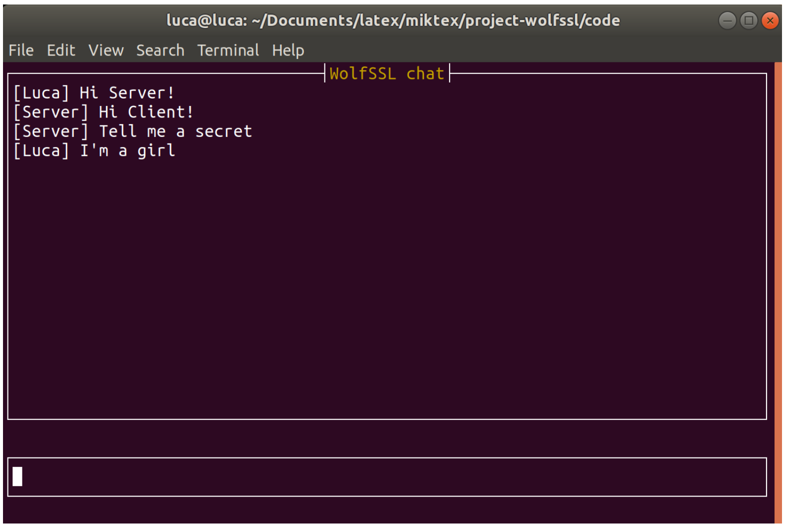


Figure 4.6: Exchange messages. Client side

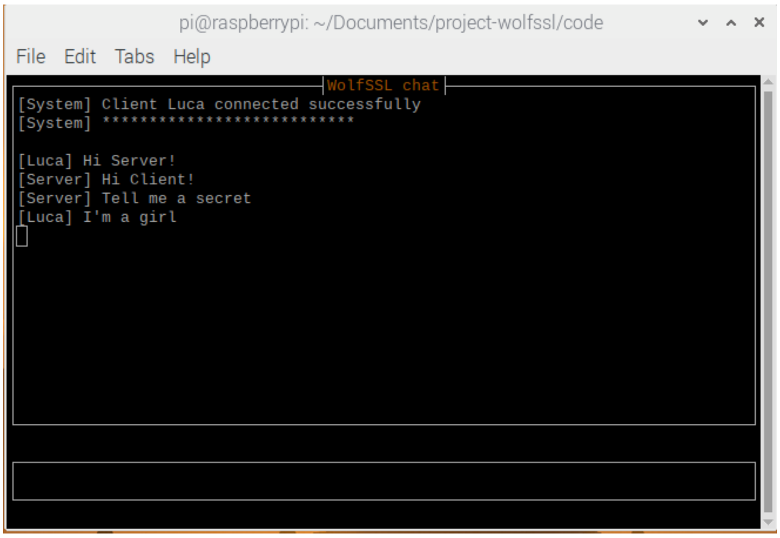
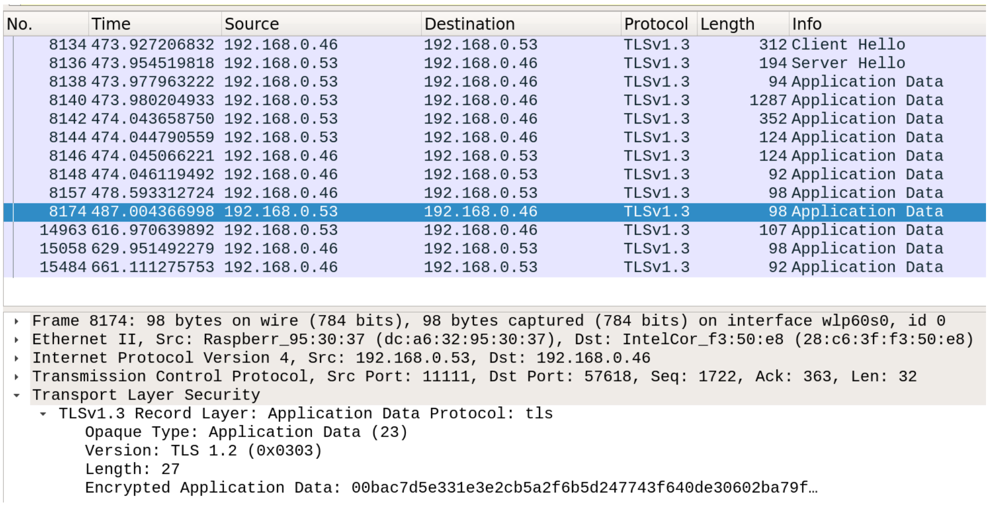


Figure 4.7: Exchange messages. Server side

As you can see, the messages are encrypted.



No.	Time	Source	Destination	Protocol	Length	Info
8134	473.927206832	192.168.0.46	192.168.0.53	TLSv1.3	312	Client Hello
8136	473.954519818	192.168.0.53	192.168.0.46	TLSv1.3	194	Server Hello
8138	473.977963222	192.168.0.53	192.168.0.46	TLSv1.3	94	Application Data
8140	473.980204933	192.168.0.53	192.168.0.46	TLSv1.3	1287	Application Data
8142	474.043658750	192.168.0.53	192.168.0.46	TLSv1.3	352	Application Data
8144	474.044790559	192.168.0.53	192.168.0.46	TLSv1.3	124	Application Data
8146	474.045066221	192.168.0.46	192.168.0.53	TLSv1.3	124	Application Data
8148	474.046119492	192.168.0.46	192.168.0.53	TLSv1.3	92	Application Data
8157	478.593312724	192.168.0.46	192.168.0.53	TLSv1.3	98	Application Data
8174	487.004366998	192.168.0.53	192.168.0.46	TLSv1.3	98	Application Data
14963	616.970639892	192.168.0.53	192.168.0.46	TLSv1.3	107	Application Data
15058	629.951492279	192.168.0.46	192.168.0.53	TLSv1.3	98	Application Data
15484	661.111275753	192.168.0.46	192.168.0.53	TLSv1.3	92	Application Data

```
Frame 8174: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp60s0, id 0
Ethernet II, Src: Raspberr_95:30:37 (dc:a6:32:95:30:37), Dst: IntelCor_f3:50:e8 (28:c6:3f:f3:50:e8)
Internet Protocol Version 4, Src: 192.168.0.53, Dst: 192.168.0.46
Transmission Control Protocol, Src Port: 11111, Dst Port: 57618, Seq: 1722, Ack: 363, Len: 32
Transport Layer Security
  TLSv1.3 Record Layer: Application Data Protocol: tls
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 27
    Encrypted Application Data: 00bac7d5e331e3e2cb5a2f6b5d247743f640de30602ba79f…
```

Figure 4.8: Application data

These are the end of communication screens from the client and from the server:

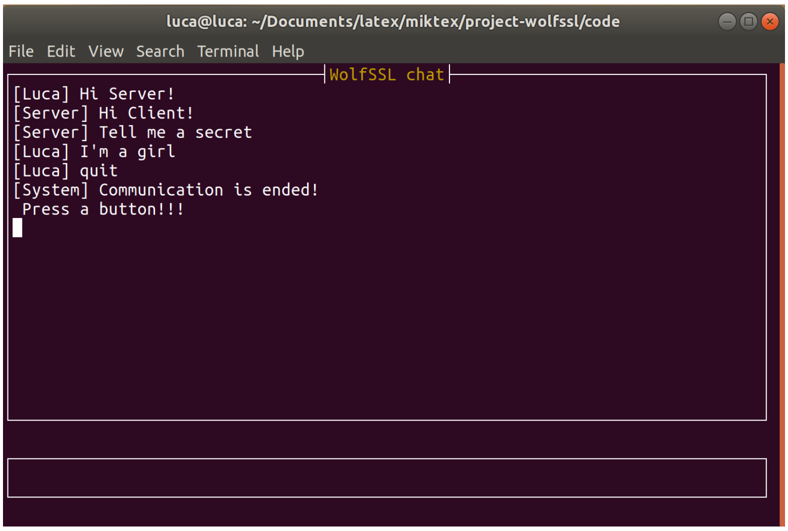


Figure 4.9: Execute WolfSSL client

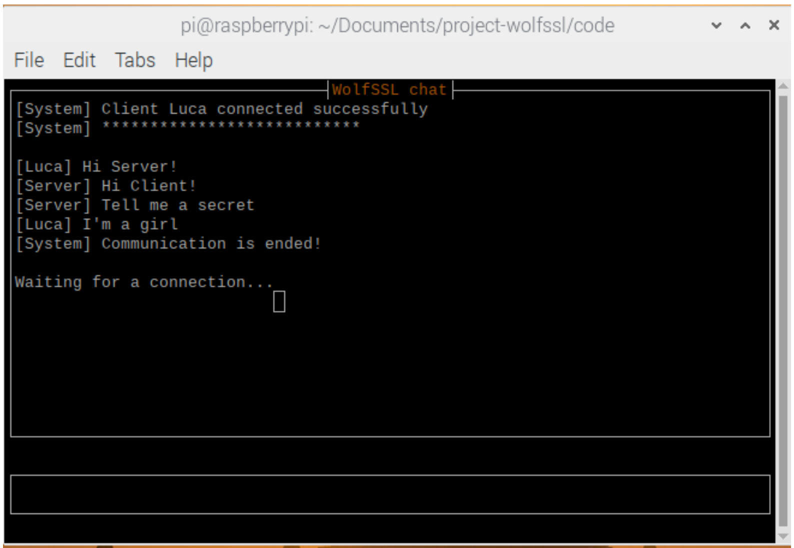


Figure 4.10: Execute WolfSSL client

************ServerKeyExchange has been removed in TLS 1.3*********

Chapter 5

Differences between WolfSSL and OpenSSL

5.1 Introduction

The main differences are:

- Memory Usage
  - WolfSSL can be up to 20 times smaller than OpenSSL; The build size is between 20 and 100 KB and the runtime memory usage between 1 and 36 KB. This gives a magior advantage of integrating in smaller embedded devices.
- Hardware Crypto
  - WolfSSL has a partnership with the most MCU manufacturers which allows to be quite early in the market to support hardware acceleration on huge list of platforms.
- Portability
  - WolfSSL is more portable than OpenSSL because is made for real-time, mobile, embedded and enterprise systems.